Centro Universitário Farias Brito

Bacharelado em Ciências da Computação

TCC

Simulador de Algoritmos de Criptografia de Cifra de Blocos com Finalidade Educacional

Tanielian Viana Barreira

Me. Sergio Araújo Yunes

Tanielian Viana Barreira

Simulador de Algoritmos de Criptografia de Cifra de Blocos com Finalidade Educacional

Trabalho de Conclusão de Curso para o curso de Ciências da Computação do Centro de Ciências Tecnológicas do Centro Universitário Farias Brito.

Centro Universitário Farias Brito

Bacharelado em Ciências da Computação

TCC

Orientador(a): Me. Sergio Araújo Yunes

Fortaleza-CE, Brasil

2020

Dedico esta labuta à todas as pessoas que sempre me zoaram...

Agradecimentos

Agradeço ao meu pai...

Por último mas não menos importantes, muito pelo contrário, aos meus professores...

Resumo

TODO: Resumo

Palavras-chave: criptografia, educacional

Abstract

TODO: Abstract

Keywords: cryptography, educational

Epígrafe (opcional, mas vai ter)

Lista de Siglas e Abreviações

3DES *Triple Data Encryption Standard*. 12

AES *Advanced Encryption Standard*. 12

CCSDS *Consultive Committee for Space data Systems*. 13

DEA *Data Encryption Algorithm*. 12

DES *Data Encryption Standard*. 12, 13, 15, 23, 24

IBM *International Business Machines Corporation*. 12

S-DES *Simplified Data Encryption Standard*. 41

Lista de ilustrações

Sumário

1 Introdução

A formação de pessoas na área de Ciência da Computação exige que as ferramentas se aproximem ao máximo da realidade existente. A academia apresenta modelos da realidade, que são possíveis de manuseio no ambiente de estudo. A visibilidade que o aprendiz precisa ter sobre o assunto em estudo deve ser semelhante àquela que será encontrada durante o seu exercício profissional. E quando essa similaridade não é encontrada, se torna difícil para o aluno visualizar corretamente em que cenário se aplica o conhecimento adquirido, quando este precisar ser utilizado (MAIA, 2001) (MAIA; PACHECO, 2003) (SILVA, 2009).

As atuais necessidades de aplicação da Ciência da Computação exigem daqueles que desenvolvem sistemas, conhecimento detalhado de como funcionam as ferramentas de trabalho, em especial os métodos e técnicas da Criptografia. Essa necessidade decorre do fato de que a *Internet*, definitivamente, está inserida na vida cotidiana das pessoas e novos costumes estão sendo adotados pela sociedade. O comércio eletrônico, as operações bancárias de transferência eletrônica de fundos, o uso do cartão de crédito como moeda de plástico, por exemplo, se constituem na realidade do convívio social. Junte-se a isso o fato de que a mobilidade na telefonia é uma realidade cristalizada entre as pessoas, independente de qual seja a sua posição social.

Por outro lado, devido à alta complexidade dos algoritmos usados nas aplicações da Criptografia (SILVA, 2009), a transmissão do conhecimento nem sempre é eficiente o suficiente, principalmente se os algoritmos forem ensinados na sua complexidade real.

O ensino nas disciplinas que envolvam a temática da segurança da informação, abordando mais especificamente o conteúdo da Criptografia – preocupação prioritária desta pesquisa – acaba sendo prejudicado pela falta de tempo hábil para discorrer sobre o assunto e de profissionais capacitados. (TODO: REFERÊNCIA) Naturalmente, a abordagem de cunho pedagógico precisa preservar os aspectos fundamentais da arquitetura de cada algoritmo.

Embora se saiba que, em nome da preservação da eficiência do trabalho acadêmico os algoritmos possam ser apresentados com alguma restrição na sua abrangência, ainda assim, é possível apresentar todo o funcionamento e implementação dos algoritmos durante o período do desenvolvimento de uma disciplina, quer no tempo destinado a uma disciplina de graduação, quer de pós-graduação, com um esforço menor do que aquele necessário para a implementação do algoritmo em sua forma original (MAIA, 2001) (MAIA; PACHECO, 2003).

Analisando o contexto acima apresentado, deriva-se a necessidade de um ins-

trumento que auxilie o processo de ensino nesta área. A finalidade deste projeto é o desenvolvimento e a implementação uma ferramenta que possibilitará a simulação do funcionamento de versões simplificadas do algoritmo criptográfico de chave simétrica conhecido como *Data Encryption Standard* (DES), para utilização de natureza pedagógica.

O produto derivado do desenvolvimento será um conjunto composto de programa ~~e documento de ensino da utilização do mesmo~~, destinados a apoiar a formação de profissionais que irão se utilizar de desenvolvedores de aplicações que utilizam algoritmos de criptografia por chave simétrica.

Essa ferramenta permitirá, então, que o algoritmo possa ser executado de modo ininterrupto, ou por etapas discretas, de modo a permitir a completa compreensão do seu funcionamento.

Diante do contexto apresentado, ressalta-se que o propósito desta monografia é contribuir para a resolução da problemática posta, motivo pelo qual define-se como objetivo geral o desenvolvimento de uma ferramenta de simulação de algoritmos criptográficos com intuito de auxiliar o processo de ensino-aprendizagem da técnica de cifra de blocos, nas disciplinas que abordem a criptografia.

Em decorrência, os objetivos específicos tem o compromisso de investigar, através de um questionário, quais as etapas dos algoritmos criptográficos baseados em cifra de blocos que geram mais dificuldades no aprendizado dos alunos; definir requisitos funcionais da ferramenta; desenvolver a ferramenta de simulação para os algoritmos *Data Encryption Standard* (DES) e *Triple Data Encryption Standard* (3DES).~~; preparar documentação sobre o funcionamento dos algoritmos e sobre a utilização do software criado.~~

Considerando que o desenvolvimento de uma ferramenta de simulação de algoritmos criptográficos é o desafio maior da pesquisa apresentada, é importante ressaltar que historicamente a criptografia por chave secreta, (utilizada nessa ferramenta), experimentou um grande impulso por volta do ano de 1974, quando foi apresentado o algoritmo *Data Encryption Standard* (DES). Trata-se de um método para a criptografia de dados baseado em cifra de blocos, que se tornou o padrão usado pelo público e, em particular, pelo governo dos Estados Unidos. Alguns documentos fazem uma distinção entre o DES como um padrão, se referindo ao algoritmo de sua implementação como *Data Encryption Algorithm* (DEA).

Esse algoritmo herdou os princípios da Cifra de *Feistel*, (1973) resultado de um projeto desenvolvido pela *International Business Machines Corporation* (IBM) sobre Criptografia por cifra de blocos. Apesar dos questionamentos sobre a sua vulnerabilidade, por conta do tamanho da chave, o entendimento de como funciona o DES transmite importante conhecimento sobre o mecanismo utilizado nas cifras de bloco.

No ano de 2001, depois de um trabalho de cinco anos, o *Advanced Encryption Standard* (AES), conhecido pela sua implementação mais famosa '*Rijndael*', em alusão

aos seus criadores, os belgas *Joan Daemen* e *Vincent Rijmen*, passou a ser o novo padrão utilizado para a Criptografia de dados. Trata-se de um método criptográfico também baseado em cifra de bloco e que, tal qual o seu antecessor DES, espera-se da comunidade científica que seja utilizado e detalhadamente analisado.

Dentre as principais características do *Rijndael* se encontra o fato de que o algoritmo ocupa pouca memória, o que o qualifica para ser utilizado em ambientes restritos, tais como telefones celulares e *smart cards*. Justamente por essas características de restrição de necessidades, esse algoritmo também é recomendado pelo *Consultive Committee for Space data Systems* (CCSDS), organização da qual faz parte o proponente do projeto.

As áreas Empresarial e Acadêmica, que se utilizam de profissionais criados na academia, possuem necessidades criptográficas (segurança nas empresas e didática nas academias) não supridas atualmente devido a falta de uma metodologia eficiente de transmissão do conhecimento para o aluno e pela dificuldade inerente a área de conhecimento citada (SILVA, 2009).

TODO: Parágrafo de finalização... Precisa?

2 Metodologia

Para se investigar quais as etapas dos algoritmos baseados em cifra de blocos que geram mais dificuldades no aprendizado dos alunos, optou-se pela metodologia de pesquisa explicativa (SEVERINO, 2018), que "além de registrar e analisar fenômenos estudados, busca identificar suas causas, seja através da aplicação do método experimental/matemático, seja através da interpretação possibilitada pelos métodos qualitativos" (p.123).

Durante a investigação, um conjunto de alunos que nunca estudou algoritmos criptográficos que usam cifra de bloco receberam um texto sobre o seu funcionamento, e foram orientados a estuda-lo e a retornarem uma avalição sobre o seu entendimento à respeito do texto, expresso por meio de formulário.

O formulário conterá um questionário sobre criptografia contendo perguntas, abertas e fechadas, voltadas a compreensão e ao nível de dificuldade do mesmo. Haverá também uma área para que os entrevistados possam explicitar suas opiniões em como um software de simulação poderia ajudar no aprendizado da criptografia.

Baseado nos formulários preenchidos pelos alunos entrevistados será melhorado o projeto do software para suprir melhor as deficiências diagnosticadas nos alunos.

Para se desenvolver o software será utilizada a metodologia Extreme Programming (XP). XP é uma metodologia de desenvolvimento ágil e foi escolhida ao tamanho do projeto, da simplicidade do escopo da solução e do tamanho da equipe. A ferramenta utilizada para o desenvolvimento será o Visual Studio 2012 Ultimate (VS 2012) e a linguagem será C#. A interface será Web (ASP.NET) e se utilizará da biblioteca Ext.Net (http://www.ext.net) para enriquecer a usabilidade do sistema.

A ferramenta de simulação poderá ser parametrizada de acordo com as necessidades do aluno e irá mudar seu funcionamento de acordo com as informações passadas por parâmetro.

Será escrito também uma documentação tanto sobre os algoritmos implementados como sobre o funcionamento do programa desenvolvido.

Será elaborado uma fundamentação teórica sobre os algoritmos que a ferramenta de simulação se propõe a implementar (DES e 3DES), abordando a História da criptografia, Cifra de Bloco, Criptografia Simétrica, Assimétrica, DES e 3DES, dentre outros. Será também analisada a existência de outras ferramentas de ensino, o que estas trazem de ganho para os alunos bem como a existência de outros simuladores cujo objetivo é melhorar o processo de ensino-aprendizagem, sejam eles voltados para o estudo da criptografia ou outras áreas da computação.

3 Fundamentação Teórica

Inicia-se com o tópico 5.1 História, onde há uma breve contextualização histórica sobre segurança e criptografia. No tópico 5.2 Criptografia, é feita uma visão geral sobre criptografia e suas aplicabilidades.

Os dois seguintes 5.2.1 Criptografia Simétrica e 5.2.2 Criptografia Assimétrica tratam de dois tipos de criptografia e explanam sobre suas definições, seus cenários de utilização, e trazem alguns exemplos de algoritmos sobre seus respectivos ramos da criptografia. O tópico 5.3 Cifra de Blocos fala sobre esse método de criptografia simétrica no qual é feita uma visão geral sobre seu funcionamento e benefícios obtidos por sua utilização.

Os tópicos 3.4 DES e 3.5 3DES tratam sobre estes algoritmos de criptografia simétrica baseados em cifra de blocos, os quais trazem uma visão geral e uma breve explicação de cada algoritmo.

No tópico 5.6 Ferramentas de apoio ao ensino, é dado uma visão geral sobre o que são e sobre o ganho que elas trazem para os alunos. O último tópico, 5.7 Simuladores voltados ao ensino, traz uma visão geral sobre simuladores e uma análise da existência de simuladores voltados ao ensino, tanto de uma forma geral como de criptografia.

Neste caso, é perceptível a intenção de trazer uma clara e breve explanação sobre os tópicos abordados neste trabalho, de forma que este se faça compreender da melhor forma possível.

3.1 História

Há algumas décadas atrás, antes que se fosse comum o uso de equipamentos de processamento de dados, a segurança da informação que era considerada importante para uma empresa se dava basicamente através de dois meios: o administrativo e o físico. Um bom exemplo para o meio administrativo é o uso de um processo de aquisição de profissionais bastante seleto e rigoroso, assim como a utilização de um contrato de confidencialidade que protege a empresa de possíveis ‘vazamentos’ de dados. Um bom exemplo para o meio físico é o uso de cofres e senhas para armazenar documentos importantes ou até confidenciais.

Com o surgimento do computador surgiu a necessidade de proteger virtualmente os arquivos, agora armazenados de forma virtual no computador. Essa necessidade é ainda mais evidente com o surgimento da Internet, que traz uma facilidade de comunicação muito grande entre os computadores.

O Internet Architecture Board (IAB) emitiu, em 1994, um relatório de título "Security in the internet architecture" (Segurança na arquitetura da Internet). O documento estabelecia que a internet necessitava de mais e melhor segurança. Entre as principais áreas citadas no relatório como sendo as que mais necessitavam de segurança estavam a infraestrutura da rede contra monitoração e controle não autorizados do tráfego da rede e também a necessidade de proteger o tráfego entre usuários finais se utilizando de autenticações e criptografias.

Com o passar dos anos, os ataques através da Internet se tornaram mais evoluídos, eles se tornaram mais automatizados e mais devastadores, necessitando cada vez mais de formas de segurança também mais evoluídas (STALLINGS, 2014).

Existe uma lista de mecanismos de segurança explicitados na recomendação X.800 (ITU, 1991). Entre eles temos a cifragem, que é melhor descrita mais adiante. A X.800 divide, muito claramente, dois tipos de criptografia, a reversível e a irreversível. A criptografia reversível é composta por um algoritmo matemático que permite que dados sejam criptografados e que estes dados criptografados possam ser decriptografados posteriormente. Já a criptografia irreversível, por sua vez, é capaz de criptografar os dados, mas a decriptografia desses dados é impossível. Esta por sua vez tem objetivos diferentes da reversível, que visa somente trafegar ou armazenar dados de maneira segura, ela é composta de algoritmos de hash e tem como objetivo autenticação e assinatura digital (STALLINGS, 2014) (ITU, 1991).

3.2 Criptografia

Segundo a National Research Council (1991, apud STALLINGS, 2008, pg. 15), "A criptografia provavelmente é o aspecto mais importante da segurança de comunicações e está se tornando cada vez mais importante como um componente básico para a segurança do computador.".

O termo Criptografia vem do Grego kryptós, que significa "escondido" e de gráphein, que dignifica "escrita". Ela é o estudo dos princípios e técnicas pelas quais os dados podem ser transformados da sua forma original em outra ilegível. Dessa forma, os dados podem ser conhecidos somente pelo destinatário, o detentor da "chave secreta", o que faz com que mesmo que tenham sido interceptados, torne difícil a leitura de seu conteúdo por alguém não autorizado. Ela faz parte da Criptologia e é um sub-ramo da Matemática (KNUDSEN, 1998).

O estudo da maneira de camuflar o real significado de uma mensagem usando técnicas e algoritmos de cifragem têm evoluído juntamente com o estudo da maneira de se conseguir entender a mensagem quando não se é o real destinatário da mesma. Este campo de estudo é chamado Criptoanálise (GAINES, 1956). A Criptologia engloba a Criptografia

e a Criptoanálise. Alguns autores se utilizam do termo Criptovirologia quando falam de vírus que se utilizam de chaves publicas (YOUNG; YUNG, 2004).

Há também a Esteganografia que não faz parte de Criptologia, mesmo sendo estudada em situações bem similares e até pelos mesmos autores. Ao contrário da criptografia que modifica a informação com intuito de transformar seu estado original em algo indecifrável a Esteganografia estuda formas de como se pode camuflar uma informação dentro de outra. Temos também a Esteganálise que está para Esteganografia assim como a Criptoanálise está para a Criptografia (SALOMON, 2005).

A criptografia se divide em Simétrica, também chamada de criptografia convencional, e Assimétrica, também chamada de criptografia por chave pública (STALLINGS, 2014) e dentro dessa divisão ainda temos algoritmos de criptografia reversíveis e irreversíveis (STALLINGS, 2014) (ITU, 1991).

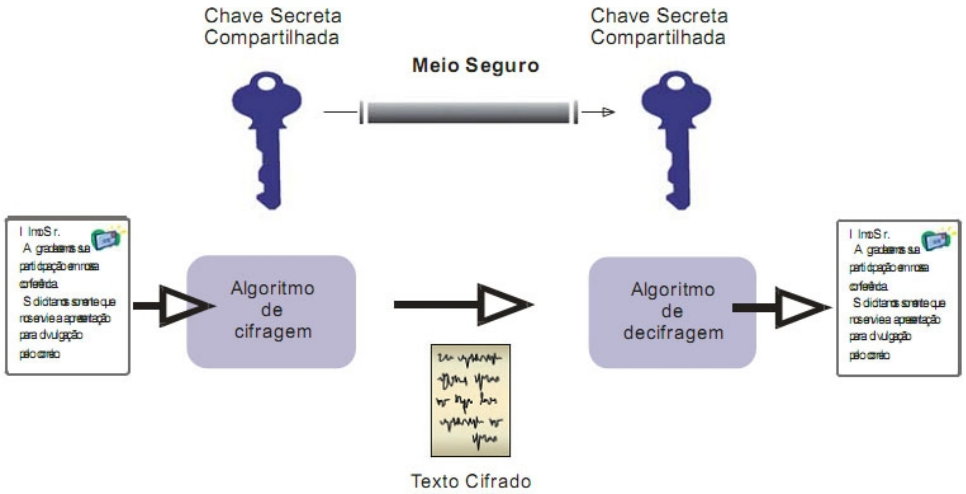
A criptografia possui inúmeras áreas de aplicação. Desde transações bancárias, envio de e-mails, segurança de arquivos sigilosos, segurança de autenticação, armazenamento de senhas em bancos de dados até o sinal de linha telefônica, sinal de TV digital e acesso a sites certificados (AVELINO; AVELINO, 2007).

3.2.1 Criptografia Simétrica

Também chamada de criptografia convencional, a criptografia simétrica é um criptosistema onde tanto a criptografia como a decriptografia são realizadas com a mesma chave.

Ela transforma uma mensagem clara em uma mensagem cifrada, usando um algoritmo de criptografia e uma chave. Esta mesma chave juntamente com a inversão do algoritmo utilizado (gerando assim o algoritmo de decriptografia do algoritmo), são necessários para que se possa obter a mensagem clara novamente a partir da mensagem cifrada, assim como demonstra a Figura 1.

Figura 1 – Criptografia Simétrica



Fonte: "Introdução à certificação digital: da criptografia ao carimbo de tempo"(BROCARDO; ROLT; FERNANDES, 2006)

Antes do computador, as cifras simétricas tradicionais poderiam se utilizar de técnicas de transposição ou de substituição, ou até as duas técnicas combinadas. Essas técnicas são os componentes básicos para todas as técnicas de criptografia.

Técnicas de transposição transpõem sistematicamente as posições dos elementos da mensagem clara. Tal técnica consiste na aplicação de alguma permutação na mensagem clara de forma que a mensagem final seja ilegível, e somente o detentor da forma de como os elementos da mensagem foram permutados pode obter novamente a mensagem de forma clara. A cifra mais simples dessa técnica é a cifra de *Rail fence*. A Figura 2 ilustra como ficaria a crifa *Rail fence* de profundidade dois do texto “Técnica de transposição”.

Figura 2 – Exemplo de *Rail fence*

```
T c i a e r n p s ç o
é n c d t a s o i ã
```

Técnicas de substituição mapeiam elementos, caracteres ou bits, da mensagem clara e as substitui por outras letras ou números ou até símbolos. Analisando a mensagem clara como sendo um conjunto de bits, então a substituição é definida pela troca de padrões de bits da mensagem clara por padrões de bits da mensagem cifrada. Como exemplo clássico temos a cifra de César, criada por Júlio César. A Figura 3 ilustra como ficaria a cifra de César com o texto “Tecnica de substituicao”.

Figura 3 – Exemplo de cifra de César

```
Alfabeto:
Claro: a b c d e f g h i j k l m n o p q r s t u v w x y z
Cifra: t u v w x y z a b c d e f g h i j k l m n o p q r s

Mensagem clara:   Tecnica de substituicao
Mensagem cifrada: Mxvgbvt wx lnulmbmnbvth
```

Existem basicamente dois os ataques possíveis em um algoritmo criptográfico. A criptoanálise, que se baseia nas características do próprio algoritmo de criptografia, e a força bruta, que engloba simplesmente repetidas tentativas de todas as chaves possíveis até encontrar a correta.

Antes da existência do computador existiam máquinas que implementavam a nível de hardware técnicas de substituição. Eram conhecidas como máquinas de rotor. Duas foram as máquinas de rotor mais conhecidas, a da Alemanha, conhecida como Enigma e a do Japão conhecida como Purple. Elas foram utilizadas durante a segunda guerra mundial e a quebra desses dois códigos pelos Aliados foi significante para o resultado da guerra. Abaixo, a Figura 4 mostra a máquina Enigma com três rotores.

Figura 4 – Imagem da máquina Enigma

Máquina Enigma com três rotores, teclado, luzes e conexões para câmbio de codificação. Fonte: Wikipedia (WIKIPéDIA, 2020)

Algoritmos simétricos são utilizados em cenários onde a mensagem tem uma necessidade de ser decriptografada, por exemplo, o Kerberos, serviço de autenticação desenvolvido no *Massachusetts Institute of Technology* (MIT) como parte do projeto Athena, que visa trazer segurança a cenários distribuídos abertos, se utiliza unicamente de cifra simétrica (STALLINGS, 2014).

3.2.2 Criptografia Assimétrica

Também chamada de criptografia por chave pública, a criptografia assimétrica é um criptosistema onde a criptografia e a decriptografia são realizadas com chaves diferentes, uma pública e outra privada. Quando uma mensagem é criptografada com uma chave,

somente a outra chave poderá decriptografar a mensagem. O criptosistema assimétrico mais utilizado é o RSA.

Ela transforma uma mensagem clara em uma mensagem cifrada utilizando uma das duas chaves acima citadas e um algoritmo de criptografia. E utilizando a outra chave citada acima e o algoritmo de decriptografia, é possível extrair a mensagem clara a partir da mensagem cifrada.

A criptografia assimétrica possui três utilizações básicas: confidencialidade, autenticação ou ambas.

A confidencialidade garante que somente o destinatário será capaz de ler a mensagem. Quando se tem essa necessidade, deve-se criptografar a mensagem com a chave pública do destinatário, enviar a mensagem criptografada para o destinatário, e ele, de posse da chave privada, poderá decriptografar a mensagem e dessa forma obter a mensagem original.

O fato do destinatário ter conseguido decriptografar a mensagem com a chave privada dele próprio garante que a mensagem só poderia ter sido decriptografada por ele, detentor da chave privada, mas não garante a identidade do remetente, visto que a chave utilizada para criptografar a mensagem é publica, assim como demonstra a Figura 5.

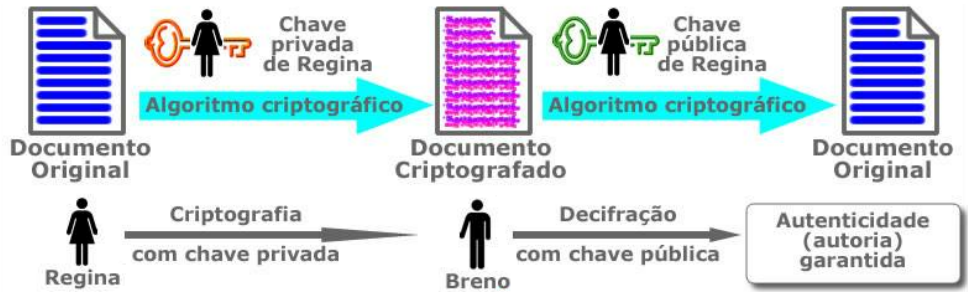
Figura 5 – Fluxo da mensagem criptografada quando o foco é confidencialidade

Fonte:

A autenticidade garante que quem enviou a mensagem foi o remetente. Quando se tem essa necessidade, deve-se criptografar a mensagem com a chave privada do remetente, enviar a mensagem criptografada para o destinatário, e ele, de posse da chave pública do remetente, poderá decriptografar a mensagem e assim obter a mensagem original.

O fato do destinatário ter conseguido decriptografar a mensagem com a chave pública do remetente comprova que a mensagem é realmente do remetente, mas não garante que o destinatário é o único que poderia decriptografar a mensagem, visto que qualquer pessoa pode possuir a chave pública do remetente, assim como demonstra a Figura 6.

Figura 6 – Fluxo da mensagem criptografada quando o foco é autenticidade

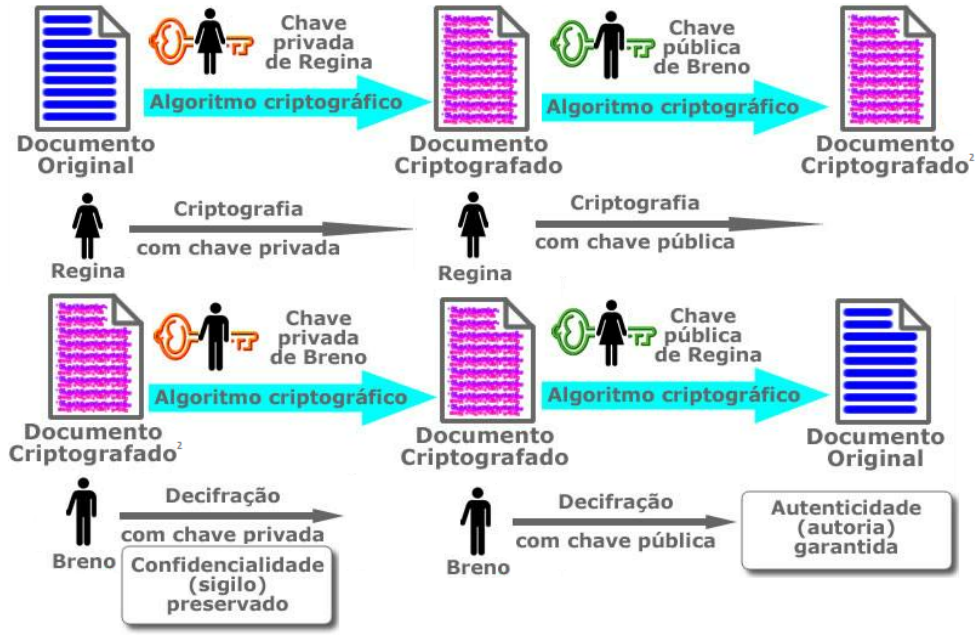


Fonte:

É possível também que se criptografe a mensagem com a chave privada do remetente, criptografar a mensagem já criptografada com a chave pública do destinatário, enviar a mensagem duplamente criptografada para o destinatário, e ele de posse da chave privada, poderá decriptografar a mensagem duplamente criptografada em uma mensagem criptografada e esta por sua vez será decriptografada com a chave pública do remetente e finalmente obter a mensagem original.

A combinação das duas criptografias, a com chave privada do remetente e com a chave publica do receptor, garante tanto que quem vai receber a mensagem é realmente o destinatário correto como garante que o remetente é quem ele diz ser (STALLINGS, 2014), assim como demonstra a Figura 7.

Figura 7 – Fluxo da mensagem criptografada quando o foco é confidencialidade e autenticidade



Fonte:

3.3 Cifra de blocos

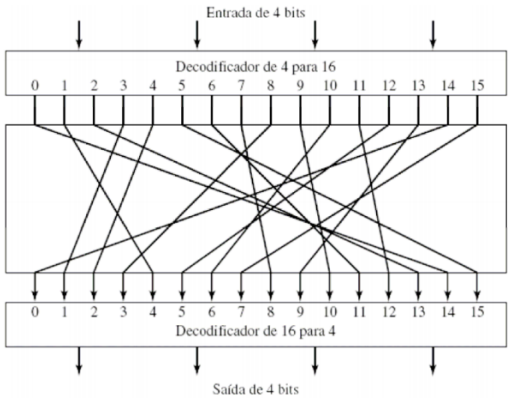
A cifra de blocos manipula um bloco da mensagem clara como um todo e utiliza este para criar um bloco de mensagem cifrada de mesmo tamanho. É comum a utilização de um bloco com 64 ou 128 bits. Uma cifra de bloco pode ser usada para alcançar o mesmo efeito que uma cifra de fluxo. Cifras de fluxo trata de certo fluxo de dados singularmente, bit a bit ou byte a byte. São implementações clássicas das cifras de fluxo as cifras de Vigenère auto chaveada e a cifra de Vernam e a mais utilizada atualmente é o RC4.

A maioria das criptografias simétricas voltadas para ambientes de rede de computadores são implementadas com cifra de blocos e grande parte dos algoritmos de cifra de bloco simétrico usados na atualidade são baseados na cifra de blocos de Feistel.

A cifra de bloco trabalha com um bloco de dados da mensagem clara de n bits para produzir um bloco de mensagem cifrada de também de n bits. Se a cifra de bloco se utilizar de um n baixo então a cifra será equivalente a uma cifra de substituição simples. E se n for grande o suficiente e ainda assim for permitida a substituição reversível entre os blocos de mensagem cifrada e não cifrada, então a mensagem clara estaria tão camuflada que a criptoanálise se tornaria inviável.

Uma cifra de substituição reversível qualquer, Feistel chamava esse cenário de cifra de bloco ideal, para um grande tamanho de bloco não é viável, do ponto de vista de desempenho e implementação, assim como demonstra a Figura 8.

Figura 8 – Cifra de bloco ideal



Texto claro	Texto cifrado	Texto cifrado	Texto claro
0000	1110	0000	1110
0001	0100	0001	0011
0010	1101	0010	0100
0011	0001	0011	1000
0100	0010	0100	0001
0101	1111	0101	1100
0110	1011	0110	1010
0111	1000	0111	1111
1000	0011	1000	0111
1001	1010	1001	1101
1010	0110	1010	1001
1011	1100	1011	0110
1100	0101	1100	1011
1101	1001	1101	0010
1110	0000	1110	0000
1111	0111	1111	0101

Fonte:

Feistel propunha que era possível chegar mais próximo da cifra de bloco ideal. Era só utilizar uma cifra de produto, ou seja, a execução de duas ou mais cifras em sequencia, tornando assim o produto final criptograficamente mais forte do que se poderia obter através de qualquer uma das cifras componentes do produto. A estrutura de Feistel consiste em repetidas rodadas do mesmo procedimento. A cada vez que o procedimento se repete é realizada a substituição em metade dos dados da mensagem sendo processados, logo após

se permuta as duas metades. A chave sendo utilizada é expandida de modo que uma chave diferente seja utilizada em cada iteração.

Na prática Fiestel propôs o uso de uma cifra que alternava entre substituições e permutações, o que na realidade é uma implementação prática do que Claude Shannon já havia proposto como, cifra de produto que alterne confusão e difusão (STALLINGS, 2014).

3.4 DES

Foi estabelecido pela IBM no final da década de 1960 um projeto de pesquisa sobre criptografia de computadores que trazia a sua frente Horst Feistel. Com a conclusão do projeto em 1971 foi apresentado como resultado um algoritmo denominado LUCIFER, que foi comercializado ao Lloyd's localizado em Londres para ser utilizado em um sistema de caixa eletrônico que também havia sido desenvolvido pela IBM. LUCIFER é uma cifra de bloco de Feistel que operava com blocos de 64 bits e se utilizava de uma palavra com tamanho de 128 bits.

Com o sucesso do LUCIFER a IBM mobilizou um novo projeto, dessa vez com o intuito de tornar o LUCIFER comercializável em grande escala, conseguindo coloca-lo em um único chip. Este projeto, que por sua vez era liderado por Walter Tuchman e Carl Meyer, contava com a ajuda tanto de consultores externos como orientação técnica da NSA. O resultado deste novo projeto foi um LUCIFER mais refinado e mais resistente à criptoanálise, mas continha um tamanho de chave de 56 bits, para poder caber em um chip.

A National Bureau of Standards (NBS), em 1973, solicitou propostas de uma cifra para ser padronizada a nível nacional. A IBM enviou o LUCIFER refinado, o que continha 56 bits, e por ser o melhor algoritmo proposto foi, em 1977, adotado como *Data Encryption Standard* (DES).

Com uma chave de 56 bits, existem ao todo 256 possíveis chaves, algo próximo de 7,2 x 1016 chaves. Aparentemente, um número tão grande de possibilidades é algo praticamente impossível de se descobrir se utilizando o método de força bruta. Por exemplo, uma única máquina processando uma criptografia DES por microssegundo levaria mais de mil anos para quebrar a cifra.

Por mais que para as máquinas de hoje, uma criptografia DES a cada microssegundo pareça irreal, pois a velocidade das máquinas de hoje já é bem superior as máquinas da década de 70, para aquela época não era algo tão simples. Mesmo assim, em 1977, Diffie e Hellman declararam que já existia tecnologia suficiente para se criar uma máquina que concentraria, de forma paralela, um milhão de dispositivos criptográficos, cada um com o poder de processamento da máquina citada no exemplo anterior. Isso reduziria o tempo de

quebra da cifra para cerca de dez horas. Infelizmente, tal configuração na época custaria em torno de vinte milhões de dólares.

Finalmente, em 1998, vinte e um anos depois, o DES provou ser inseguro, quando a Eletronic Frontier Foundation (EFF) anunciou que tinha quebrado uma cifra DES utilizando uma máquina "decifradora de DES" montada por menos de 250 mil dólares. Como se isso já não fosse suficiente para tornar o DES um algoritmo criptográfico ultrapassado, ainda existe a constante evolução do hardware, aumentando cada vez mais a velocidade de processamento e consequentemente possibilitando tanto que o método da força bruta seja mais viável, temporalmente falando, como também que sejam criados algoritmos de criptografia que se utilizem melhor desse novo poder de processamento.

Felizmente já existem várias alternativas para o DES, entre elas estão o Advanced Encryption Standard (AES) e o Triple DES (3DES) (STALLINGS, 2014).

3.5 3DES

A criptografia múltipla é quando um algoritmo de criptografia é utilizado repetidas vezes. Primeiramente, a mensagem clara é criptografada utilizando um algoritmo de criptografia. A mensagem cifrada é então usada como entrada para um algoritmo de criptografia, podendo ser o mesmo utilizado anteriormente ou algum outro algoritmo, e esse processo pode ser repetir por indefinidas vezes.

O Triple DES (correlacionar com 3DES) é um exemplo de criptografia múltipla. Ele se utiliza do algoritmo DES três vezes, usando duas ou três chaves diferentes.

Em seu estado inicial a criptografia múltipla possui dois estágios, no caso do DES duplo, cada um se utilizando de uma chave diferente uma da outra.

No caso do DES duplo a criptografia E de uma mensagem M se utilizando de duas chaves K1 e K2 resultando em um texto criptografado C seria assim:

C = E(K2, E(K1, M))

Já a sua decriptografia D seria assim, aplicando as chaves inversamente:

M = D(K1, D(K2, C))

O DES triplo veio como uma alternativa clara para sanar o problema do DES simples, gerado pelo avanço computacional, uma vez que aumenta o custo do ataque da mensagem clara conhecida para 2112 (quando se utiliza de duas chaves) o que está além do possível, pelo menos, atualmente. Mas se utilizar de três estágios com três chaves diferentes exige um tamanho de chave de 168 bits (56 x 3), o que pode ser custoso.

Para diminuir o problema citado, Tuchman propôs uma alternativa se utilizando somente de duas chaves:

C = E(K1, D(K2, E(K1, M)))

A solução acima apresentada se tornou relativamente popular tendo sida adotada para uso nos padrões de gerenciamento de chaves ANS X9.17 e ISO 8732.

Atualmente contra o 3DES não existem ataques criptoanalíticos práticos, visto que, o custo de uma pesquisa de chave por força bruta seria de ordem 2112 (quando fossem utilizadas somente duas chaves) o que é equivalente a aproximadamente 5 x 1033.

Mesmo o 3DES com duas chaves sendo de difícil ataque, ainda pode haver uma certa preocupação. Portanto pesquisadores creem que o melhor seria se utilizar do 3DES com três chaves. Como já dito anteriormente o 3DES com três chaves possui uma chave de tamanho efetivo de 168 bits, o que a torna mais segura em relação com o de duas chaves, e possui a seguinte forma (STALLINGS, 2014):

C = E(K3, D(K2, E(K1, M))

3.6 S-DES

O S-DES é uma versão simplificada do algorítimo DES (Data Encryption Standard).

Ele se utiliza de parâmetros de entrada menores que os possíveis com o DES e faz somente 2 permutações, tornando assim este o melhor candidato para análise quando o objetivo é aprendizado.

Continuar...

3.7 Ferramentas de apoio ao ensino

A educação abrange dar e receber conhecimento. Qualquer sociedade possui esse cenário, que é responsável pela manutenção e propagação às gerações que se seguem, da cultura necessária à convivência de um membro na sua sociedade (HAMAWAKI; PELEGRINI, 2009).

Dentre as formas de aprendizagem, são citadas duas teorias importantes por Ausubel (AUSUBEL; NOVAK; HANESIAN, 1980), a aprendizagem significativa e a mecânica.

A primeira diz respeito à ideia de que a aprendizagem é um processo por onde uma informação recém-adquirida relaciona-se com um aspecto importante da estrutura de conhecimento do aluno, ou seja, quando a nova informação adquirida vincula-se em conhecimentos relevantes previamente adquiridos na estrutura cognitiva do aluno. A aprendizagem significativa é onde o aluno realmente aprende.

A aprendizagem mecânica por sua vez ocorre quando o novo conhecimento se associa pouco ou não se associa a algum conhecimento importante já existente na estrutura

cognitiva do aprendiz. Quando isso ocorre o conhecimento adquirido recentemente é gravado de maneira arbitrária. Essa aprendizagem é inviável quando um aluno recebe um novo conhecimento em uma área de conhecimentos nova para ele. Ou seja, aprendizagem mecânica acontece somente até que alguns elementos do conhecimento pré-adquirido, relevantes a novas informações na mesma área de conhecimento, existam na estrutura cognitiva do aluno e possam ser utilizadas como base para a aprendizagem significativa. E é através dessa aprendizagem que se inicia a criação, na cabeça do aluno, de uma estrutura cognitiva mais complexa, onde ele deixa de aprender de forma passiva e mecânica e passa a assimilar o conteúdo de forma mais clara e não linear (AUSUBEL; NOVAK; HANESIAN, 1980).

Existe um problema comum entre professores e alunos de disciplinas do curso de Ciência da Computação, e este é: Existe uma dificuldade em demonstrar a real dinâmica dos eventos computacionais. Por melhor que o mestre possua conhecimento e comunicação, que o aluno dedique raciocínio e atenção, a total compreensão dos conceitos abordados fica comprometida pela forma de abordagem das disciplinas.

O computador não deve ser o substituto do professor, mas sim, tomar o papel de ferramenta educacional auxiliando o aprendizado. Com isso o papel do professor passa a ser mais produtivo.

Primeiramente, ferramentas voltadas ao ensino, já se utilizando do computador, se baseavam na máquina de B. F. Skinner, onde se utilizava a ideia de instrução programada, que consistia de dividir o conteúdo total em pequenas partes lógicas e sequenciais.

Somente durante a década de 1960, foi dado inicio ao conceito de Computer Aided Instruction (CAI), ou seja, Programas Educacionais por computador (PEC). A real dispersão do CAI só aconteceu com popularização dos microcomputadores, possibilitando assim, a criação de diversos tipos de ferramentas de ensino, como, tutoriais, exercício-e-prática, avaliações, jogos, e simulações (HAMAWAKI; PELEGRINI, 2009).

3.8 Simuladores voltados ao ensino

Algumas situações são tão singulares, que se preparar para tais torna-se difícil. E portanto, com o intuito de proporcionar a alguém um conhecimento maior sobre estas situações os simuladores foram criados.

A simulação é uma representação do mundo real. As primeiras simulações foram criadas com o intuito de disponibilizar um ambiente seguro para situações que envolvessem risco ao humano. Dentre elas podemos citar simulações de viagens e mergulhos profundos. Posteriormente, foram criadas com o intuito de se obter uma economia, seja ela de tempo e/ou dinheiro, que é o caso da indústria automobilística e aviação.

Diversas são as áreas de conhecimento que fazem uso das simulações (BANKS *et al.*, 2009). Na ciência da computação há uma disponibilidade de simuladores, cada um atendendo a uma respectiva disciplina, assim como redes de computadores, arquitetura de computadores, técnicas de programação e sistemas operacionais.

Os simuladores possuem um potencial bem maior do que as outras ferramentas de ensino citadas acima. A aplicação de simulações no universo acadêmico permite que o aluno desenvolva hipóteses, teste-as, analise os resultados e concretize seus conhecimentos. Simuladores devem ser utilizados como ferramenta complementar as aulas lecionadas pelo professor.

Mesmo com todas as vantagens envolvidas, o desenvolvimento de um simulador não é algo trivial. Uma vez que a ferramenta possui um cunho pedagógico, a utilização de recursos multimídia para tornar a simulação mais fiel à realidade é muito importante, e a utilização destes recursos não é algo de simples desenvolvimento.

Quando o aluno possui pouco conhecimento na área, os simuladores são indicados como melhor ferramenta de auxilio. Principalmente, se forem para auxiliar cursos de extensão e graduação (MAIA, 2001) (MAIA; PACHECO, 2003).

Até o final da escrita desse documento o único simulador de criptografia gratuito que foi encontrado foi o Enigma Simulator by Terry Long (http://www.terrylong.org/), e este, se concentra apenas na simulação do algoritmo da máquina Enigma utilizada na Alemanha no período da segunda guerra mundial.

4 Ferramenta desenvolvida

Nesse capítulo descrevo o **simulador de algoritmos de criptografia com finalidade educacional** desenvolvido no decorrer da escrita desse trabalho de conclusão de curso.

4.1 Informações técnicas

4.1.1 Requisitos funcionais

O simulador deve ser disponibilizado ao usuário através da internet pelo link: *https://cryptoedu.netlify.app/*

(Pode-se estender. Não priorizei pois falaste que não era tão importante no momento)

4.1.2 Requisitos não funcionais

O simulador deve ser visualizado em qualquer browser (contanto que esteja na última versão oficial).

(Pode-se estender. Não priorizei pois falaste que não era tão importante no momento)

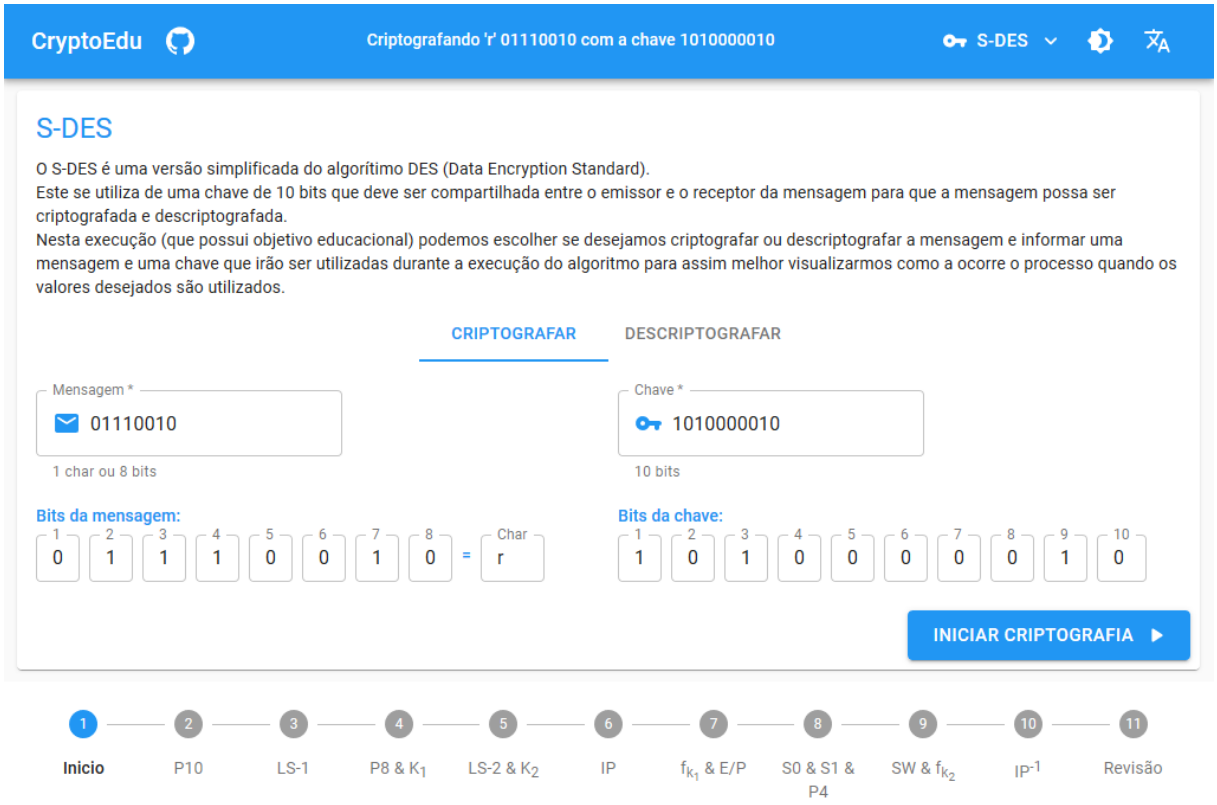
4.1.3 Ator

O público alvo da ferramenta são os alunos de Computação, mas os atores desta não estão limitados à. Todos que desejam aprender como a criptografia de cifra de blocos funcionada, refinar e/ou lapidar os conhecimentos já adquiridos ou até somente desmistificar esse conteúdo complexo chamado criptografia.

4.2 Estrutura da interface

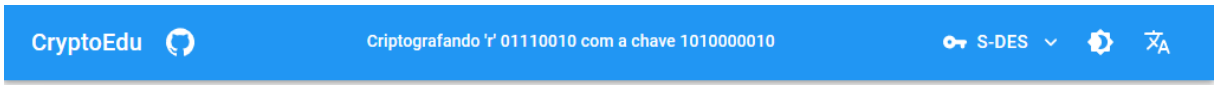
Nessa seção descrevo os elementos contidos na interface de maneira estrutural.

Figura 9 – Estrutura da interface



4.2.1 Cabeçalho

Figura 10 – Cabeçalho

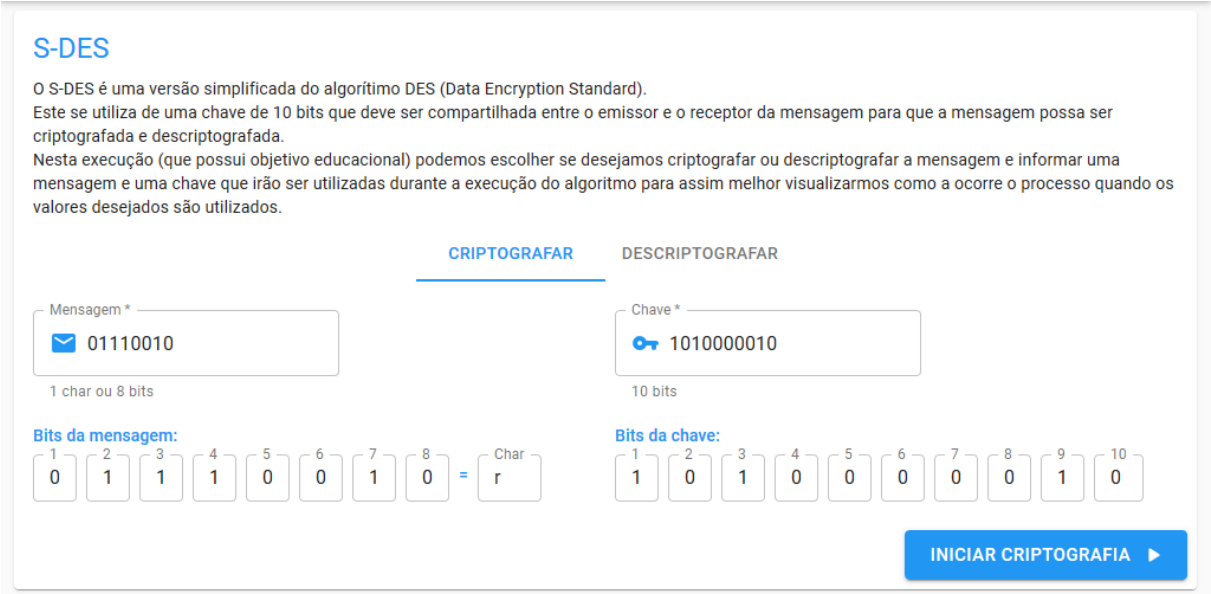


A região do cabeçalho possui:

- O nome do simulador: **CryptoEdu**.
- Link do repositório onde está localizado tanto o código da ferramenta como o TCC: *https://github.com/TanielianVB/CryptoEdu*
- Descrição dos valores passados como entrada para o algoritmo em execução.
- *Combo Box* de escolha do algoritmo que está em execução.
- Botão para alternar entre o tema **claro** e **escuro**.
- Botão para alterar o idioma no qual o simulador está sendo exibido.

4.2.2 Conteúdo

Figura 11 – Conteúdo



A região principal do site será onde cada passo da execução do algoritmo selecionado irá ocorrer.

Inicialmente irá conter uma interface discorrendo sobre o algoritmo selecionado e posteriormente cada passo que estará sendo executado. É possível navegar por esses passos através dos botões de navegação exibidos na parte inferior da região de cada passo.

4.2.3 Rodapé

Figura 12 – Rodapé

A região do rodapé contém:

- Todos os passos necessários para a execução do algoritmo em execução.
- Quais passos já foram completados.
- Qual passo o usuário se encontra no momento.
- Quais passos ainda faltam ser completados para finalizar a execução do algoritmo.

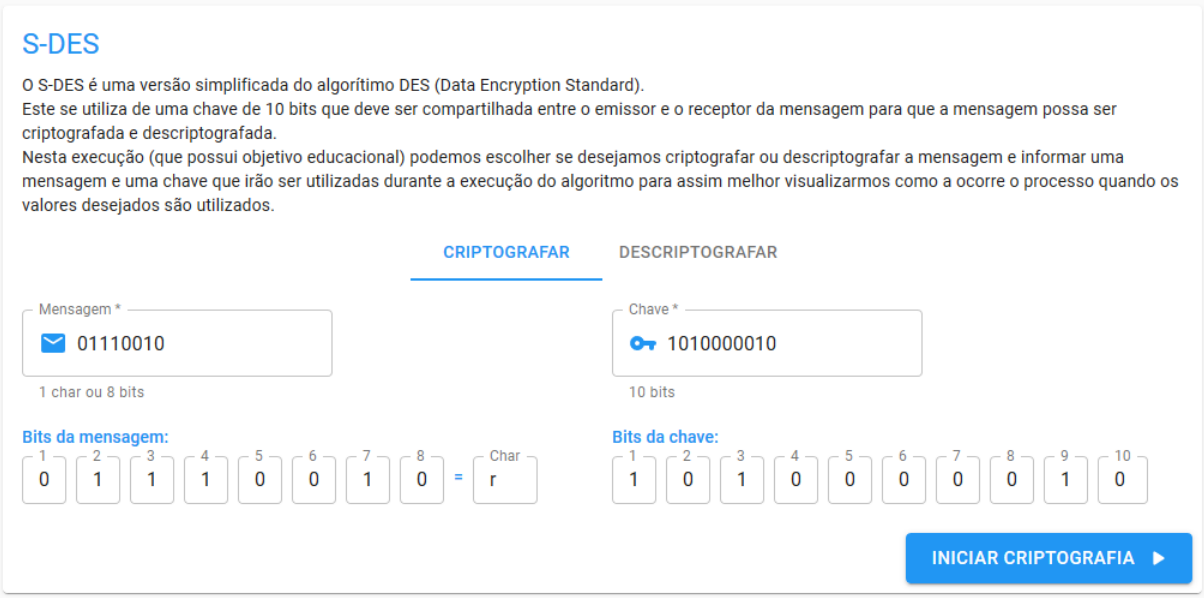
É possível também, a qualquer momento, navegar para qualquer passo diretamente. Basta-se clicar sobre este.

4.3 Interface do conteúdo

Descrição da interface apresentada em cada um dos passos da execução do algoritmo.

4.3.1 Tela inicial

Figura 13 – Tela inicial - entrada de dados



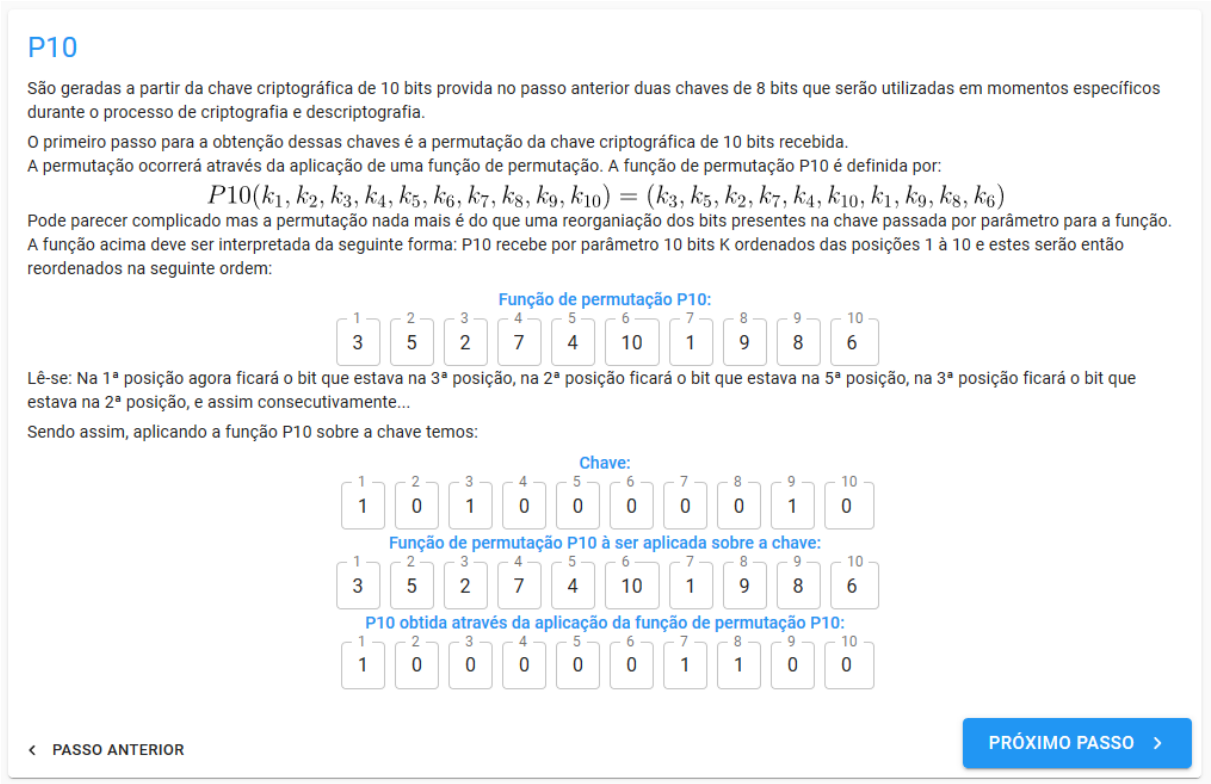
A interface inicial faz uma breve descrição do algoritmo selecionado na *Combo Box* de escolha de algoritmo buscando situar o usuário no contexto selecionado para execução.

O usuário pode então escolher se ele deseja o fluxo de execução **criptografar** ou **descriptografar** e assim então informar valores customizados para os campos **Mensagem** (**Mensagem cifrada** caso o fluxo escolhido tenha sido o **descriptografar**) e **Chave**.

Os algoritmos recebem como entrada bits. Por conta disso, são exibidos os bits contidos nos campos e que serão utilizados para a execução do fluxo escolhido. Tanto para facilitar o preenchimento do campo **Mensagem** como para melhorar a compreensão do usuário sobre o valor contido no campo, é possível informar no campo uma letra, visto que essa pode, e é, facilmente convertida para 8 bits. Isso ajuda não somente no preenchimento do campo durante a execução do fluxo **criptografar** mas também na validação do resultado obtido da execução do fluxo **descriptografar** visto quê é possível, mais facilmente, comparar as mensagens (tanto a de entrada do fluxo **criptografar** quando a de saída do fluxo **descriptografar**) se estas forem letras. Exemplo: A letra **'T'** gera a sequência de bits: **01010100**.

4.3.2 Passo P10

Figura 14 – Passo P10 - Permutação de 10 bits

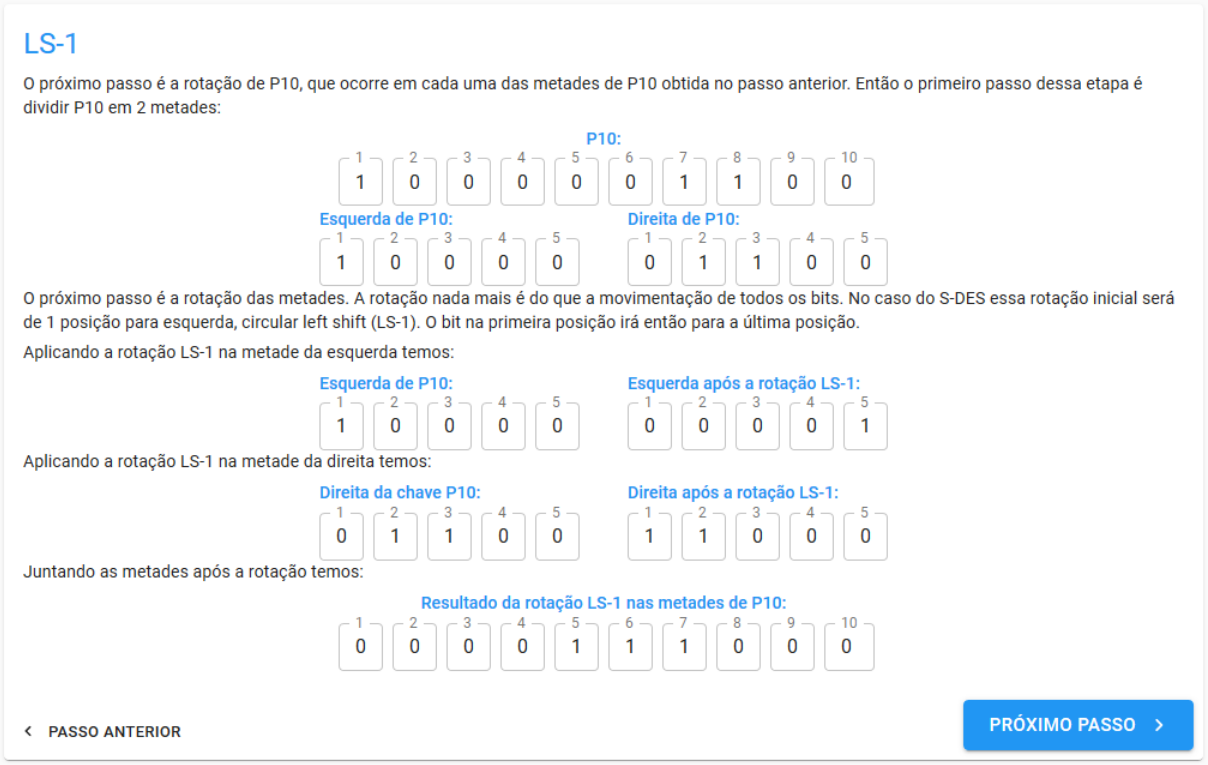


A interface do passo P10 contextualiza o objetivo pelo qual esse passo existe, explica a definição de uma função de permutação, apresenta a função de permutação P10 (incluindo função matemática) e explica como esta deve ser interpretada.

Somente então, após tal contextualização, que se exibe a chave entrada como parâmetro para o fluxo em execução (visto que ela é o parâmetro de entrada da função), a função de permutação P10 que será aplicada sobre esta e por fim a chave obtida de resultado após a aplicação da função de permutação P10.

4.3.3 Passo LS-1

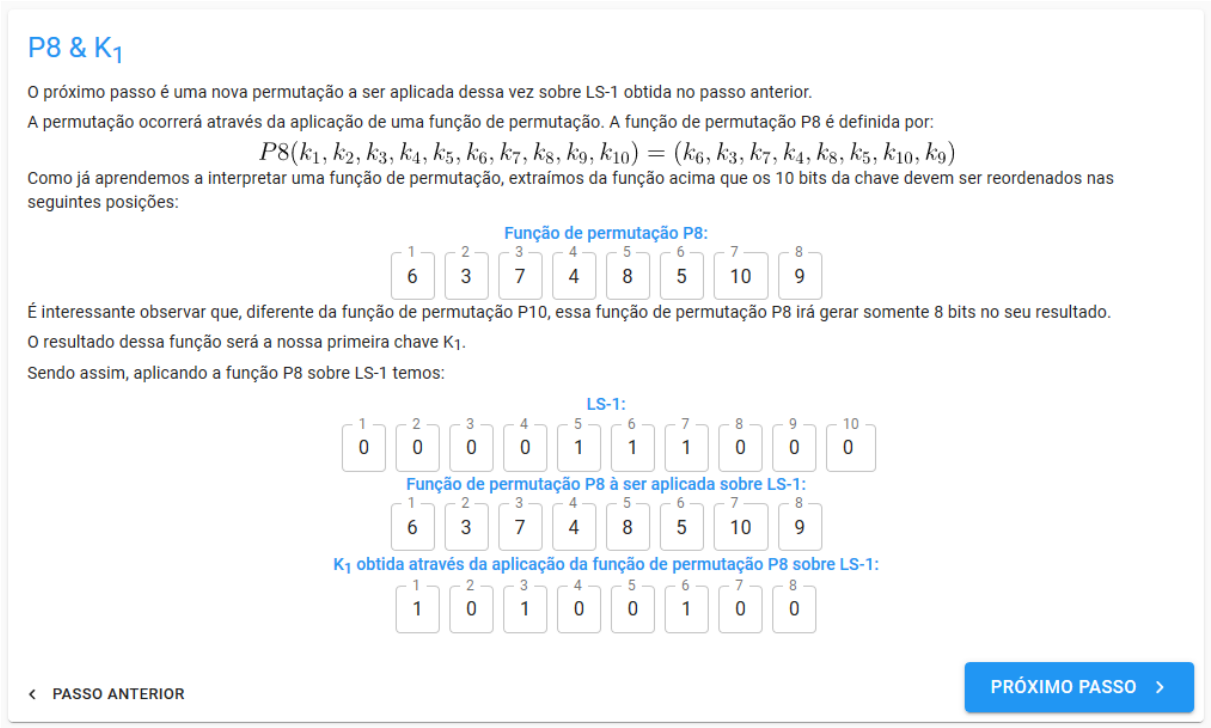
Figura 15 – Passo LS-1 - circular left shift de 1 posição



A interface do passo LS-1 demonstra como o processo de rotação deve ocorrer. Incluindo a divisão do valor obtido no passo anterior (P10), o que é o processo de rotação, a aplicação desse processo nas metades e junção das metades para obtenção do resultado.

4.3.4 Passo P8 & K1

Figura 16 – Passo P8 & K1 - Permutação de 8 bits e geração da primeira chave K1

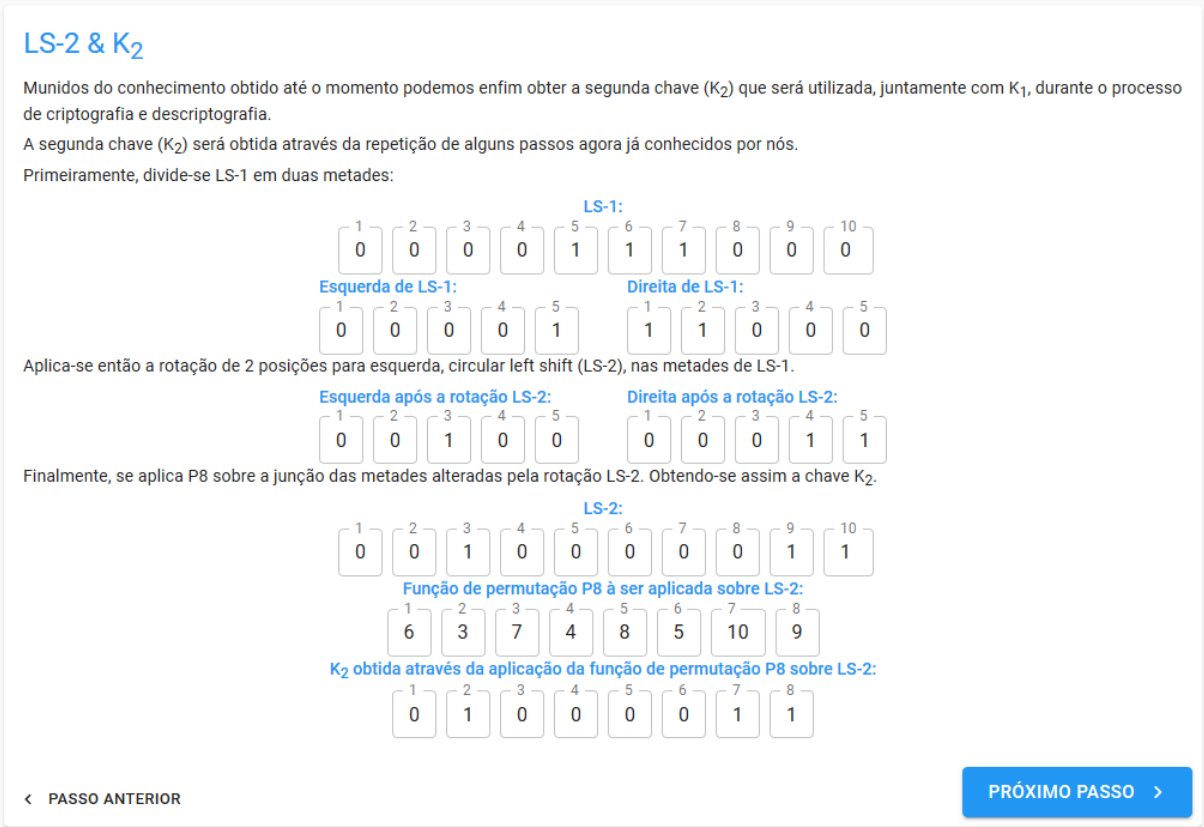


A interface do passo P8 & K1 apresenta a função de permutação P8 (incluindo função matemática), exibe a chave LS-1 obtida na rotação anterior (visto que ela é o parâmetro de entrada da função), a função de permutação P8 que será aplicada sobre esta e por fim a chave K1 obtida de resultado após a aplicação da função de permutação P8 sobre LS-1.

Essa interface é a primeira que parte do princípio que o usuário já possui algum conhecimento prévio, sendo este adquirido no passo P10, que é o conhecimento sobre funções de permutação.

4.3.5 Passo LS-2 & K2

Figura 17 – Passo LS-2 & K2 - circular left shift de 2 posição e obtenção da chave K2

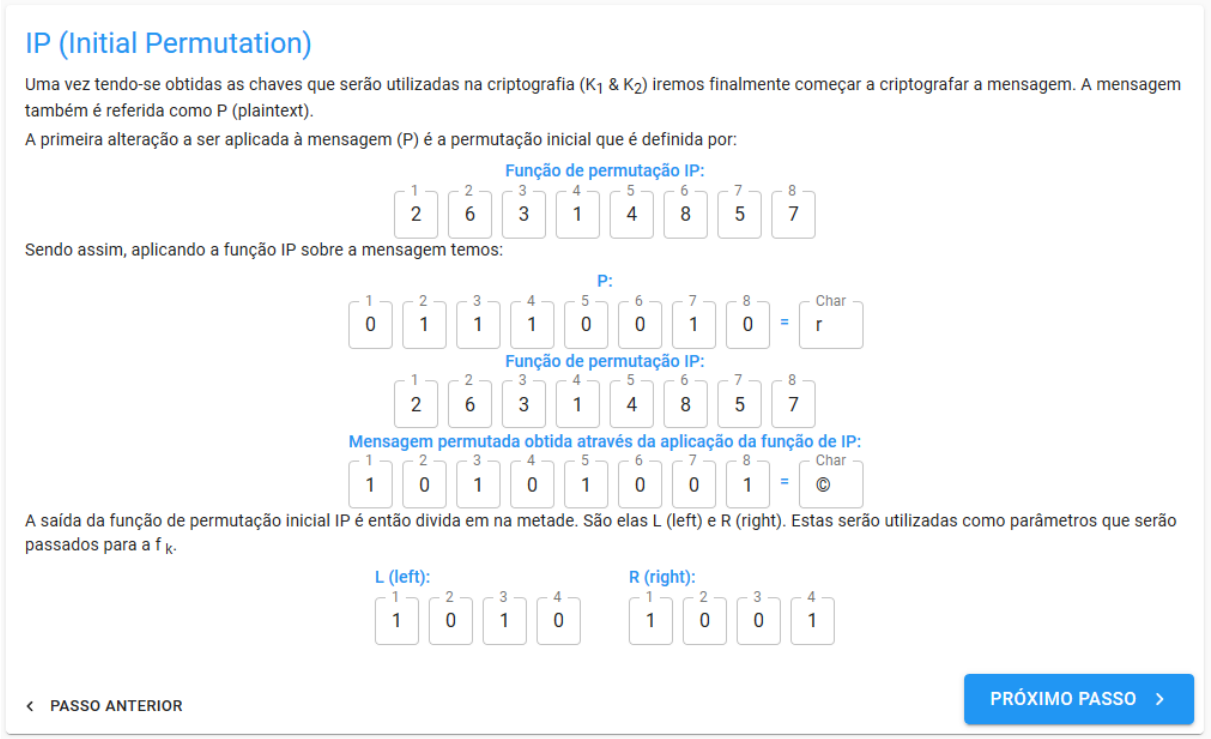


A interface do passo LS-2 & K2 explica como obter a chave K2, que consistem em dividir o resultado do passo LS-1 em duas metades, aplicar o processo de rotação, dessa vez rotacionando 2 vezes, em cada metade obtendo-se assim LS-2 e finalmente aplicar a função de permutação P8 em LS-2 culminando em K2.

Essa interface exige, além do conhecimento exigido na interface anterior, a ciência de como o processo de rotação funciona, tendo este sendo obtido no passo LS-1.

4.3.6 Passo IP

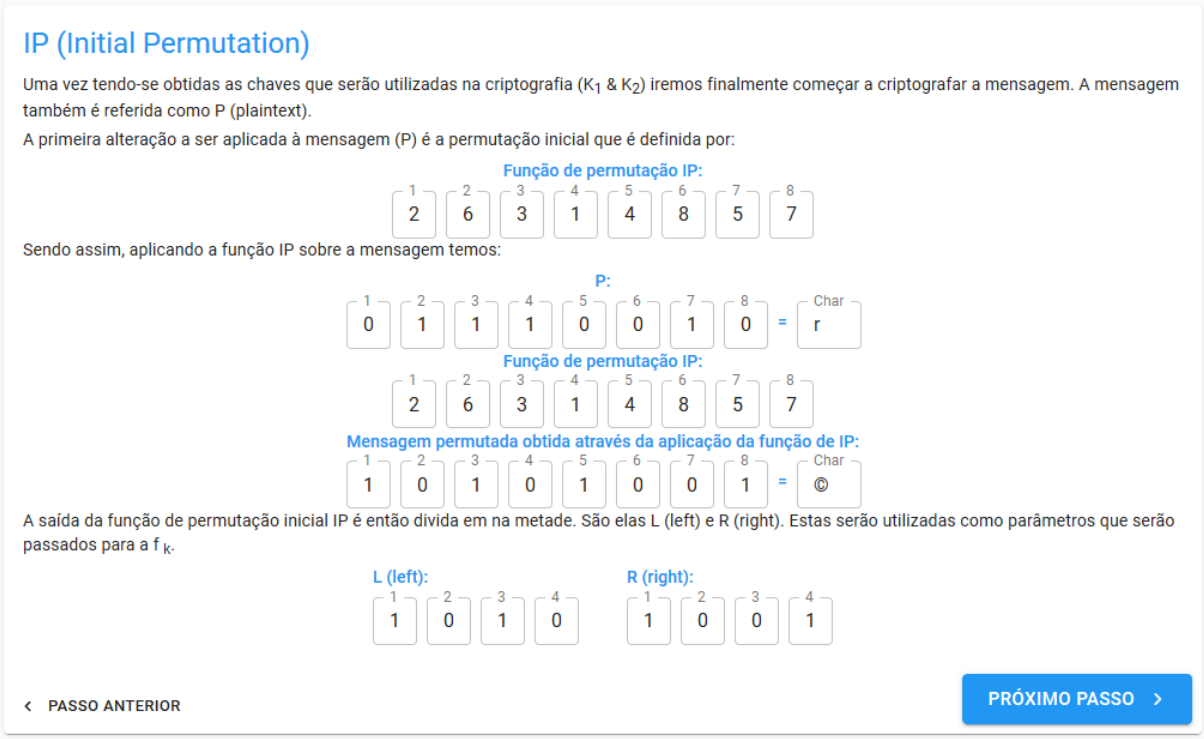
Figura 18 – Passo IP (Initial Permutation) - Permutação Inicial



Escrever...

4.3.7 Passo fK1 & E/P

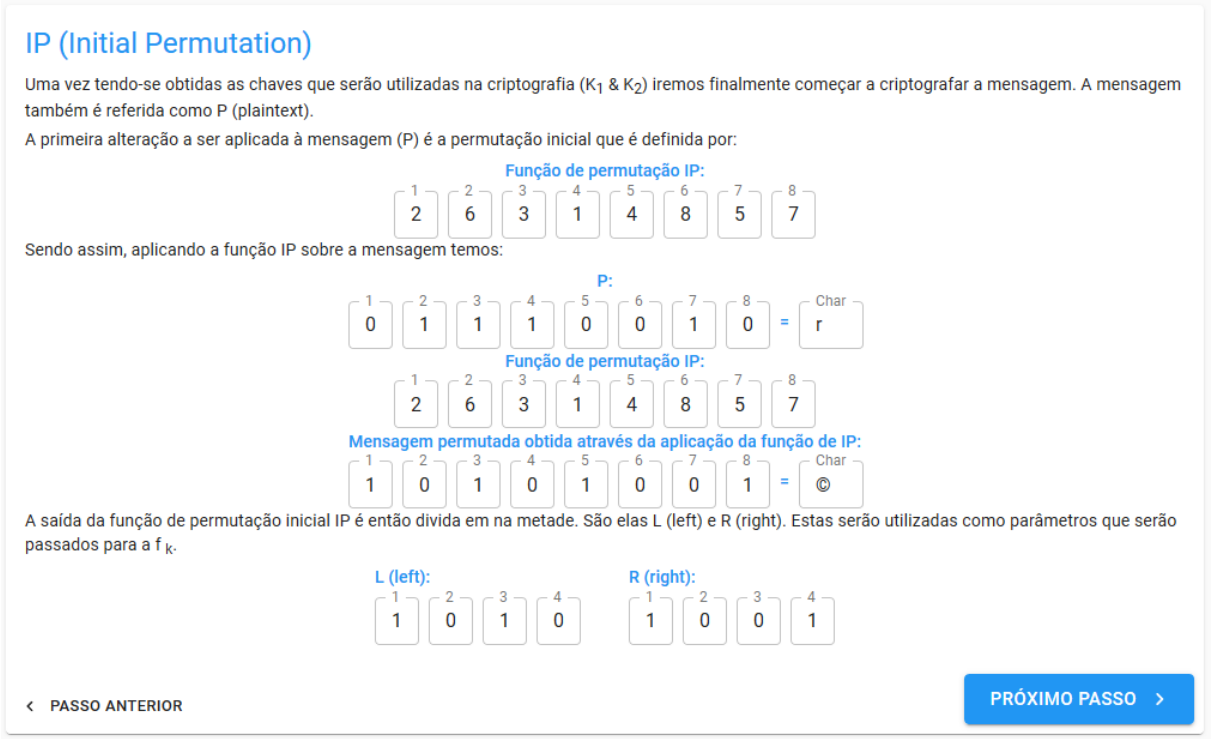
Figura 19 – Passo fK1 & E/P (Expansion/Permutation)



Escrever...

4.3.8 Passo S0 & S1 & P4

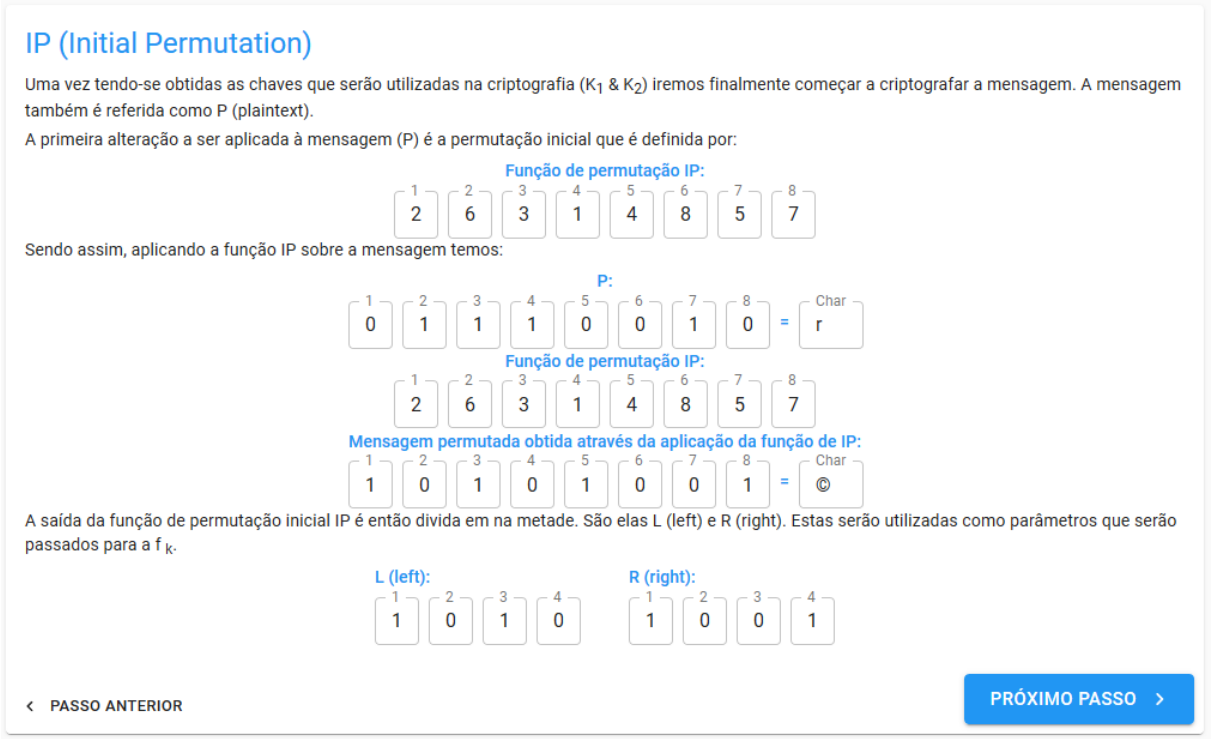
Figura 20 – Passo S0 & S1 & P4



Escrever...

4.3.9 Passo SW & fK2

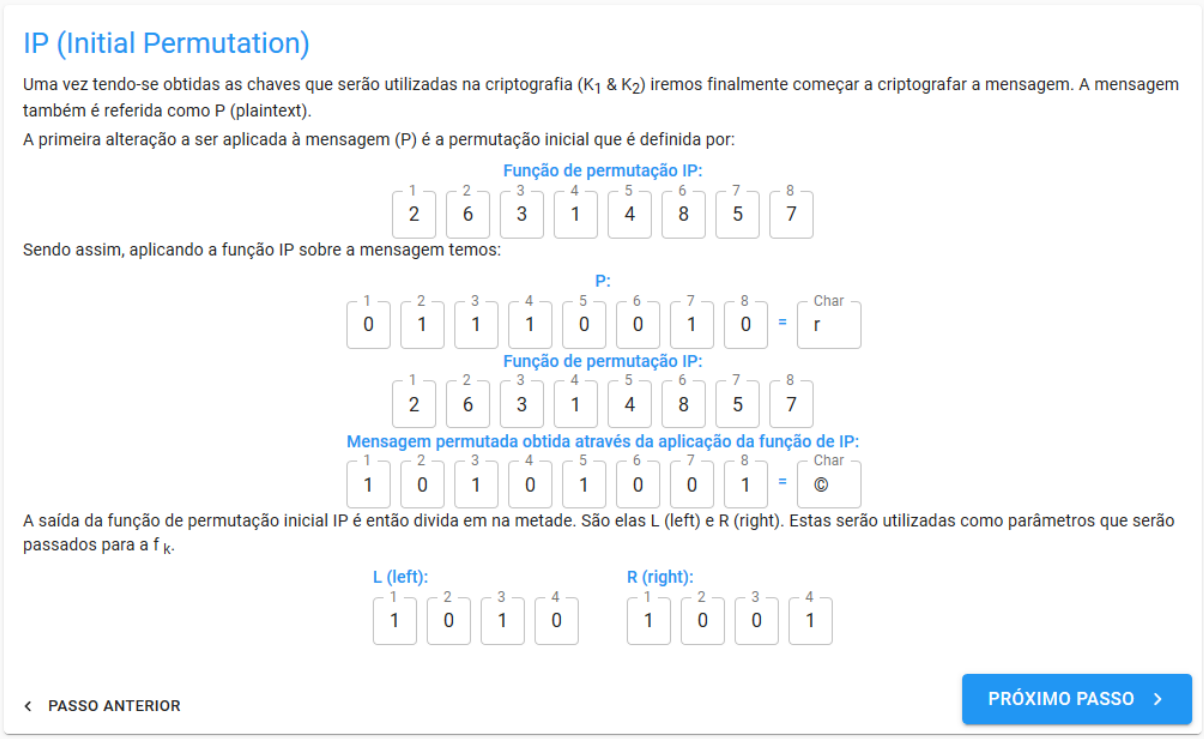
Figura 21 – Passo SW & fK2



Escrever...

4.3.10 Passo IP-1 (Inverse Initial Permutation)

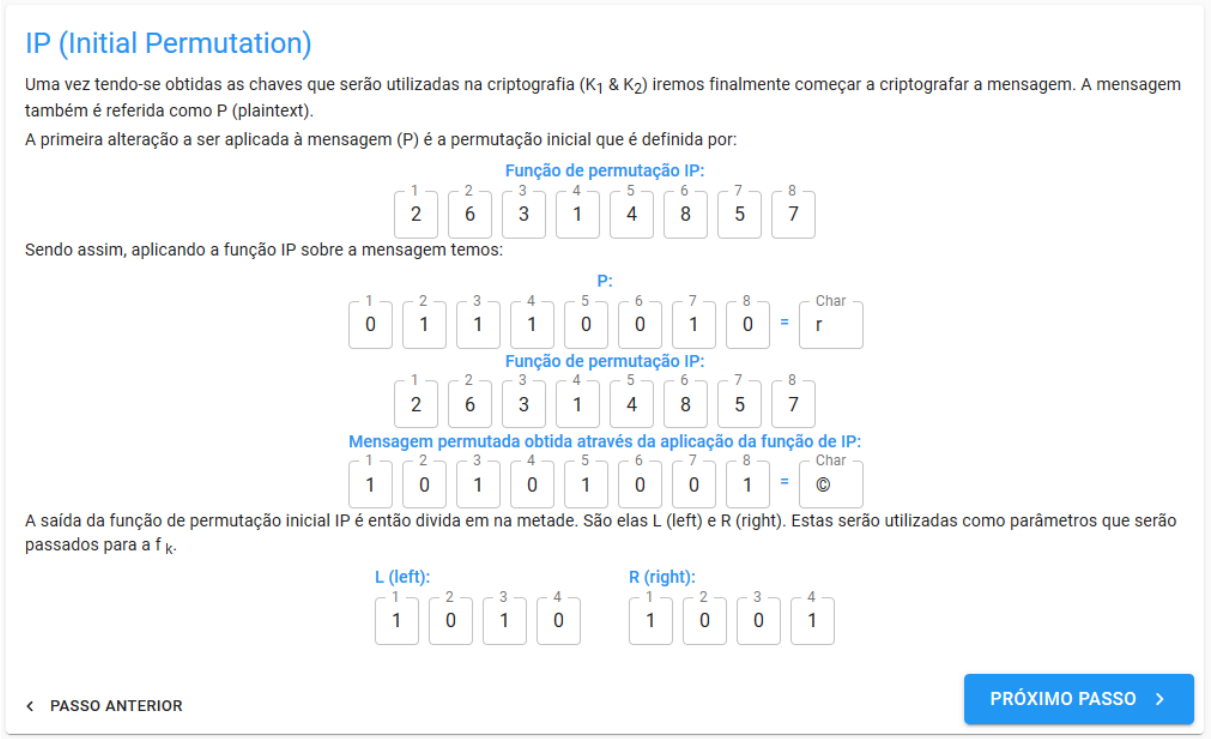
Figura 22 – Passo IP-1 (Inverse Initial Permutation)



Escrever...

4.3.11 Passo Revisão

Figura 23 – Passo Revisão



Escrever...

4.4 Limites da solução

A ferramenta foi desenvolvida prevendo uma fácil extensão das suas atuais funcionalidades. Mas, visto que o escopo do projeto pode, facilmente, se exceder além do limite possível de execução de um trabalho de conclusão de curso, alguns limites foram impostos para viabilizar o desenvolvimento da ferramenta em tempo hábil. São eles:

- Somente 1 algoritmo será disponibilizado. Sendo este, o *Simplified Data Encryption Standard* (S-DES).
- Só estará disponibilizado no tema **claro**.
- Só estará disponibilizado em **Português-BR**.

5 Pesquisa com os alunos

TODO: Coninuar...

5.1 Perguntas

TODO: Coninuar...

6 Conclusão

TODO: Coninuar...

7 Contribuição e trabalhos futuros

TODO: Coninuar...

Referências

AUSUBEL, D. P.; NOVAK, J. D.; HANESIAN, H. Psicologia educacional. 2. ed. [S.l.]: Interamericana, 1980. ISBN 8520100848. 25, 26

AVELINO, D.; AVELINO, I. C. Aplicações da criptografia em ambientes computacionais. In: . [S.l.]: IV SEGeT – Simpósio de Excelência em Gestão e Tecnologia, 2007. 17

BANKS, J. *et al.* Discrete-Event System Simulation. 5. ed. [S.l.]: Prentice Hall, 2009. ISBN 9780136062127. 27

BROCARDO, M. L.; ROLT, C. R. D.; FERNANDES, R. Introdução à certificação digital: da criptografia ao carimbo de tempo. BRy Tecnologia, 2006. 18

GAINES, H. F. Cryptanalysis: a study of ciphers and their solution. [S.l.]: Dover Publications, 1956. ISBN 9780486200972. 16

HAMAWAKI, M. H.; PELEGRINI, C. de M. As ferramentas do ensino a distância e suas contribuições para a eficácia no processo de aprendizagem do aluno. CEPPG - nº 21, p. 84 à 91, 2009. ISSN 1517-847. 25, 26

ITU, I. T. U. Security architecture for open systems interconnection for CCITT applications: Recommendation X.800. [S.l.]: The international telegraph and telephone consultative committee - CCITT, 1991. Geneva. 16, 17

KNUDSEN, J. Java Cryptography. [S.l.]: O'Reilly, 1998. 16

MAIA, L. P. SOsim: Simulador para o ensino de sistemas operacionais. Dissertação (Mestrado) — Universidade Federal do Rio de Janeiro - UFRJ, 2001. 11, 27

MAIA, L. P.; PACHECO, A. C. A simulator supporting lectures on operating systems. 33'd ASEE/IEEE Frontiers in Education Conference, 2003. 11, 27

SALOMON, D. Coding for Data and Computer Communications. [S.l.]: Springer, 2005. ISBN 9780387212456. 17

SEVERINO, A. J. Metodologia do trabalho científico. [S.l.]: Cortez, 2018. 14

STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. [S.l.]: Pearson, 2014. 16, 17, 19, 21, 23, 24, 25

WIKIPéDIA. Enigma (máquina). Wikipédia, 2020. Disponível em: <https://pt.wikipedia.org/wiki/Enigma_(máquina)>. 19

YOUNG, A.; YUNG, M. Malicious Cryptography: Exposing Cryptovirology. [S.l.]: Wiley Publishing, Inc., 2004. ISBN 9780764549755. 17